intelligence, the IMPACS system **200** can be taught to cache frequently used images or perform other access optimizations to improve performance even more.

[0339] The IMPACS system **200** is vastly different both in concept and in execution from conventional prior art approaches. The differences include at least the following:

[0340] Explicit Patient Unification for Interoperability. The IMPACS system **200** addresses a limitation of DICOM which is the non-global uniqueness of the patient identifier tag (PatientID) across images. Patient unification is a complex process that will vary depending on what types of slave PACS servers **110**$_n$ are being unified. Different techniques for unification will typically be needed based on the circumstances, geographic region, legal regulations etc. The IMPACS system **200** can handle a variety of mechanisms for patient unification be it using a separate subsystem or even a manual process. The unification provides the IMPACS system **200** with a specific patient's PatientID DICOM identifiers across all the slave PACS servers **110**$_n$ that are part of its network. With this information, the IMPACS system **200** can permit any authorized user to access all the images he is permissioned to see for a given patient across all the provider (slave) PACS servers **110**$_n$ exactly as though these images were all resident on the IMPACS system **200** itself. This will happen without any rewriting of any image tags in the slave PACS **110**$_n$.

[0341] Centralized and not Peer-To-Peer Design. Contrary to conventional approaches, the IMPACS system **200** inserts its central intelligence between every relevant modality M$_n$, workstation WS$_n$, user U$_n$ or any other client connecting to any of its component slave PACS servers **110** and the former do not peer with any of the slave PACS servers **110**. In an implementation, it is not possible for any agent connected to the IMPACS system **200** to access any of the slave PACS servers **110**$_n$ except through the IMPACS system **200** itself, coming under its authentication and security frameworks. The connected entities are not even aware that the slave PACS servers **110**$_n$ even exist. Even in emulation mode **300** where the IMPACS system **200** behaves like one of the slave PACS servers **110**$_n$ it does not require that the actual slave PACS server **110** be connected, online or that it even actually exist, nor does this matter to the connecting agent. The emulation functions **300** provided by the IMPACS system **200**, pertain to authentication and patient identifiers used for the images rather than explicit peering to a slave PACS server **110** and as such, the IMPACS system **200** can directly emulate the slave PACS server **110** (and its storage) internally in its software if needed. The image store in this context might be in a connected, yet separate database that may not even be able to function as a PACS server **110** except when serving images through the IMPACS system **200**.

[0342] Centralized Roles and Permissioning. By defining its own user identities, roles and permissioning (maps **518** and **520**) which map into the slave PACS server's **110** authorizations, the IMPACS system **200** can support a wide variety of granular or hierarchical access to its slave PACS server's **110** data. In fact, the IMPACS system **200**, with some configuration, can operate with any authorization or permissioning pro-

tocol that might be desired as long as the users and agents defined by such a scheme can be mapped into appropriate image permissions at the slave PACS servers **110**$_n$. Known prior art approaches either do not directly address permissioning at all or suggest a framework for a doctor to request patient authorizations for image access. In the latter case this permissioning has to be done at the level of every hospital where the patient P$_n$ has images, effectively on a peer-to-peer basis and the onus is on the doctor to determine all the locations at which the patient's images are. For a patient P$_n$ with a common name like John Smith this should prove a herculean task. The IMPACS system **200** is designed to handle roles, access and permissioning across all hospitals within its own framework for all agents connected to it. It can tie easily into a specialized permissioning system to manage permissions as well if needed.

[0343] Complete Monitoring and Audit Trail of All Access. Since all access to any images has to go through the IMPACS system **200**, the IMPACS system **200** can maintain a comprehensive audit trail and manage access at any level of granularity desired. As such, the IMPACS system **200** can also constantly monitor its connections for unusual access or hacks in a way that prevents any user, modality or workstation from bypassing such monitoring. Such an extensive degree of auditing, which might be needed for compliance with various government legal requirements for medical data, is simply not possible in conventional PACS systems **100** without adding on non-standard frameworks for the same.

[0344] Extensible DICOM Tag Intelligence to Permit Wider Use. The central engine of the IMPACS can seamlessly handle DICOM tag modification, patient anonymization etc. all of which can be done on the fly on image delivery to the user U$_n$/workstation WS$_n$ without modifying the images stored in the slave PACS servers **110**$_n$ at all. This can all be done by additions to the IMPACS system **200** logic, programming its brain/control engine **201** appropriately, without the need to create any new infrastructure, network links etc. Put differently, once the core IMPACS system **200** is in place, it can handle most use cases that one can envision for DICOM images across a variety of potential users. Thus, the IMPACS system **200** can deliver images to radiologists with full patient information, to researchers with patient anonymization, to insurers with additional patient tags as needed regarding their insurance identifiers etc. All this can be done using the same tag database obtained from the slave PACS servers **110**$_n$ when the IMPACS system **200** was set up. None of the conventional approaches to DICOM interoperability provides these features.

[0345] Modality and Device Monitoring to Enable New Methods for Image Storage and Retrieval. The IMPACS system **200** can be extended to analyze images and detect if they are from devices such as smart phones and cameras rather than medical modalities. The IMPACS system **200** can be programmed to provide custom DICOM tags for such images to permit storage in a slave PACS server **110**. The IMPACS system **200** can detect the type of workstation that is using the final requested DICOM image and the speed